Application Architecture Overview

BombBomb Video for Salesforce

Authentication:

OAUTH 2.0.

Authorization:

Role and permission-based access to prevent unauthorized access to your data.

- IAM roles
- Custom ACLs

Change Management:

The entire build and deployment ecosystem is governed by a gating process that is enforced, including:

- Peer code review for secure coding practices
- QA testing and automated testing for application functionality

Cloud Security:

Application is cloud hosted and uses a multi-tenant architecture.

Compatibility:

Works directly inside Salesforce Enterprise and Unlimited editions using Lightning.

Continuous Monitoring:

Monitoring, alerting, and centralized log and event management.

- On-call security team monitors all Web Application activity through a SIEM
- 24/7 application performance monitoring
- Monthly pentesting performed by IT staff
- Routine third-party security reviews and pen tests
- Log aggregation and retention for compliance

Data Privacy:

BombBomb collects lead and contact emails and records ID's for the purpose of creating tracking events within the Salesforce Org. When sending emails through BombBomb, the sent email is stored in the BombBomb account. All videos are stored in BombBomb's servers for serving the content to recipients and tracking interactions.

Data Security and Integrity:

Communication protocols are encrypted using TLS 1.2 over public networks. Data at rest is encrypted using a minimum of AES 256. A Bastion Host also governs all access to customer production data.

Private Subnet:

All endpoints sit behind a subnet to protect against attack.

- MFA required for access to customer production data
- VPN IP restrictions are enforced to allow access to authorized team members only